CHINA INFOWORLD

中國計算機報

1996 合订本

网络篇

《中国计算机报》

一九九六年合计本 （上）

网 络 篇

出 版 说 明

《中国计算机报》是中国计算机行业的权威媒体，它充分贴近广大厂商和最终用户，迅速报道最新行业动态和技术热点，有很强的时效性和实用性，受到读者的好评。鉴于用户在保存报纸时有很大困难，将报纸的有珍藏价值的文章汇集成册，是广大读者的迫切要求，当然也是我们义不容辞的责任。

《中国计算机报》(1996 年合订本)应运而生，它汇集了报纸 96 年全年的精华，我们按照网络和计算机软硬件使用技巧将其分为上、下两大篇章。

网络篇中既有对网络热门技术评介，又有对各领先厂商产品的评测，所涉及产品和技术包括 ATM、TCP/IP、Java、Internet、FDDI、Ethernet、FastEthernet 等等，另外，在本书中你还可以发现这些网络技术产品在中国各行业的应用实例。

计算机软硬件使用技巧篇更是包罗万象，不仅有 Windows 95、DOS 6.22、Novell Netware 等流行软件平台下的使用技巧，还有大量文章涉及了 Unix/Xenix、VMS 系统的应用，其中关于 WPS、UCDOS、Word、Excel、Powerpoint、FoxPro、病毒防治、Netscape、Xing 等软件的使用技巧更有极强的实用性，而有关 UPS、显示器、终端、主机板、打印机、串行设备、硬盘、键盘的使用与维修方面的文章，一定能帮助你解除在计算机使用中出现的烦恼。

为读者提供最优秀的文章是我们的一贯宗旨，我们欢迎您对我们的工作提出宝贵意见。

《中国计算机报》编辑部

一九九七年四月

□报社地址：北京昌平沙河定泗路信苑　□国内统一刊号：CN11－0004

□定价： 48 元(上、下册)

目　　录

三位 Internet 创始人
Vinton Cerf、Bill Joy、Tim Berners－lee 谈
Internet 未来像

Internet 向何处发展？某些专家预测，Internet 网及其核心部分的 World Wide Web 到本世纪末将拥有 10 亿个用户。这是吹牛还是希望？为弄个明白，美国《信息周刊》(Information Week)直接走访了 Internet 网的三个开创人：Vinton Cerf、Bill Joy 和 Tim-Berners－Lee。Cerf 现任 MCI 公司数据结构部资源副总经理和 Internet 协会主席，该协会负责制定网络标准、协议和实施办法。Joy 是 Sun Microsystems 公司创始人之一和研究部副总裁。Berners－Lee 现任 W3C 大学联盟协定主席，W3C 大学联盟协定是挂靠在麻省理工学院(MIT)的正式 Web 标准组织。这三位 Internet 的先驱人物向信息周刊杰出撰稿人 Larry Lange 就下列问题发表的看法如下：

1、Internet 向何处发展？

Cerf：看来，家庭将配备连接大部分用具的 LAN，这样电力公司就能调整供电高峰的需求，并能对计算机控制设备的运行进行远程诊断。Internet 的服务将很容易存取，并可和电视服务进行交互工作。计算机软件将帮助建立家庭电视会议，支持 远程计算，并能进行多方参加的比赛。

我们还认为将出现对 Internet 的财政支持问题，而且现金支付也许终将成为 Internet 网络经营的一个组成部分。教师和家长能用电子邮件交换意见，从而纨绔子弟也不能谎称无家庭作业。借助于装有数字式无线电的笔记本计算机对 Internet 进行移动存取将成为家常便饭。

红外通信将可用于局部连接，因此讲演者可自动地将其笔记、图表卸到学生的笔记本计算机上。各种商务卡将可用笔记本计算机之间的无线通信所代替。坐下来面对面开会的人们也将用这种方式立即连到“Internet”。当然，在这种环境里安全性将是十分重要的问题。

Joy：我认为 Internet 可能将首先用于商业市场，然后进入家庭。在商业市场上，公司要发布信息。因此，光是散发信息就有很多事要做。如果你看一下像娱乐、教育或信息高速公路之类的商业市场，那你就必须要弄清信息的价值是体现在“让人拥有它”。这或许就是一般的推销作用或广告作用。事实上，通过做广告让人得到信息，你也要花印刷费。

Berners－Lee：1994 年 7 月我在日内瓦 举办了第一次 World Wide Web 会议，想引导开发商重视开发虚拟现实产品。特别是想推动从现有的静态图象向全部虚拟现实的方向逐渐发展，所以在较慢机器上的编程使用较慢的通信线路，也能解决他们处理的某些虚拟现实世界的表现手法问题。

2、Internet 的商业化程度？

Joy：人人都想做那件事，即成为 Internet 的首家银行：“记录下信用卡，并收取手续费。”我们正注意你服务器中需要何种技术，我们还在与政府研究，以保证电子商务协议的开放性，使我们不致于有首家垄断“网络银行”的名声。

Cerf：基础设施总必须要有自身的支持，即便它是靠纳税的方式，否则它就不能存活。Internet 不同于道路系统，它能够并且应该作为一种有生命力的商业服务来收费。有些特殊的商业市场需要帮助，而这可由政府或其它支持机构来提供。总的说来，提倡服务竞争似乎仍为最有吸引力的方式。

Berners－Lee：Internet、特别是 Web 正从出现时的一种纯应用发展为我们进行通信、学习、计算和商业的潜在的信息空间。很多公司参加 W3C 是因为他们要求那种空间稳定可靠，并有所发展。他们认识到，Web 作为一条高速公路和一个市场，必定会成为使其产品有竞争力的开路先锋。

3、Internet 网络的安全性问题多大？可能会有什么解决方案？

Joy：我们正试图要解决这个技术问题，且在探求：“我们如何制造有生命力的、安全的服务器，同时能保存交往中人的匿名和私人问题中的某些地址？”

我也认为防火墙是很重要的，因为网上总会出现一些抢劫者。没有防火墙，我们也不能连到网上，这是由于这个内部网络对我们的商业非常重要的缘故。

Cerf：MCI 公司市场部通过可在 Internet 上做生意而大胆地朝增加 Internet 存取附加值的方向努力。

我们将同我们的合伙人和商业用户一道工作，帮助他们使用 Web 技术提供市场形象及在全球安全环境下的财务交易支持。

我们的目标是要把 Internet 引向一般公众，并使它深深扎根于繁荣新产品、新服务和新商业的沃土之中。

4、在 Internet 成为一种家庭的日常应用之前还需要些什么？

Berners－Lee：显然，我们需要一个用拨入 PPP［点对点协议］存取的大市场，在每一个地区都有大量兼容的 PPP 或 SLIP［串行线 Internet 协议］的提供者。我们可假定，Web 浏览器和 TCP［传输控制协议］软件将与现在的任何一种操作系统捆绑在一起，如 IBM 的 OS/2 Web Explorer 和 Windows 95。

终端设备仍是十分昂贵的，尽管我期待着某一天我女儿的粮食口袋里会有一台 1000 象素×1000 象素的彩色显示器。

Cerf：我们都清楚需要提供保障 Internet 存取安全的较好工具。这就允许公司和个人用户保护其内部资源，同时又允许他们向外延伸并能够出现在全球的 Internet 网上。我们也发现了多种新的应用，如包方式语音、包方式视频、广播和举行多方会议、游戏等等，需要扩展基础的“最大努力”的包方式服务。

隐私问题正越来越引起人们的关注，并需要加以解决。建立一个 10 亿用户网络的路径选择系统是一个严重的挑战。

另一个问题是移动存取。我认为这种技术的成本正在很快降低，不出 10—15 年、或许更短时间会解决这个问题。例如，在发展中国家里蜂窝式电话服务现在发展得相当快，PC 机和 LAN 在这些国家也迅速被采用。

5、有没有出现有信息和无信息的事，如果有，则将是个问题吗？

Cerf：虽然这是件我们极力要避免的事，但我认为我们在存取信息时总会有某些缺口。人们希望 Internet 的存取将是普遍可用的，并且它的很多信息都将是不用附加费就能提供的。

图书馆的存取现已做到这一点。例如，在 Maryland 州，正出现的“免费网络”是地方补助的，连到了 Internet 网，并还在连接一些当地的公告板系统。

总是会有一些有奖服务，但我认为这不是一个必然的结论，即我们将弥补这个有无信息的缺口。

Joy：现在，有一个问题是，如果你要看 Web 的内容，那么实际上你需要 56kbps 的速度。因此我们要研究信息压缩问题，使人们能以 14.4kbps 的速度就能看 Web 内容，或以不昂贵的调制解调器或袖珍 PC 机就能做到这一点。

6、Sun 和 MCI 公司找到了适合不同要求的办法了吗？

Joy：围绕着公司网与公用网的差别，你有很多事可做。在公司方面，我们 Sun 公司在这里正做的一件事就是科罗拉多州 Aspen 的一个项目，并提出这问题：“我们需要为这些社团、家庭、学校和市政府提供什么样的服务？”但这是个完全不一样的问题，因为坦率地说，在家的人就没有像他们在公司一样有连网和获得信息的能力。如工作时，每人都会有台工作站或一台带网络的 PC 机。

Cerf：MCI 公司自从进入 NSFNet［国家科学基金会网］的骨干网以来，已参与对科学和研究团体提供 Internet 服务。MCI 对这方面的贡献是很多的，如设备、服务和现金。它将其高频宽带设备用作 4 兆位传输的研究，最近还同其它公司一道参与帮助将学校和图书馆接入 Internet。MCI 公司理解公共服务的意义和重要性，所以它现在以及将来的服务都是为了未来的发展。

MCI 公司也是 Internet 协会的创始成员之一，它对 Internet 协会的理事会全力支持并提供财政支持。

7、“World Wide Web”这个名字是怎么来的？

Berners－Lee：当然，World Wide Web 这名字是一目了然的，“Web”一词是指非集中式的、非层次化的拓扑技术。Web 前面用“WorldWide”可能比用“Global”更好些。因此在早些时候，人们称它是一项大工程，且有了这样一个名字，以后也许再也不会去掉了。

（第一期）

PEM：Internet 电子邮件安全标准

王勋华

一、PEM 的安全服务范围和内容

PEM(Privacy－Enhanced Mail)是 IRTF(Internet Resource Task Force)的隐私与安全研究小组完成的一个电子邮件方面的安全标准。PEM 的目的就是尽可能地从电子邮件的细节方面独立出来，成为一个能与诸多电子邮件软件相接口的标准。

总的说来，PEM 具有如下的特点：基于网络应用层；基于端对端(end－to－end)的操作方式；尽可能地与 MTA 相兼容；与很多用户代理相兼容。

1. PEM 安全机制

PEM 所提供的安全机制包括：

(1)加密，即通过对报文进行加密变换，这样信道上传送的是一些毫无意义的字符，从而达到安全传送的目的。

(2)报文发起方认证，即对报文发送者的身份进行认证，避免有人冒充的可能性。

(3)报文完整性测定，它主要保证报文在传送过程中不被篡改(增加或部分删除)。

(4)报文发起方的不可否认性，它主要保证用户在发送某一邮件后不能否认。只有用户采用公开密钥密码体制时，PEM 才提供这种服务。

(5)密钥管理(key management)，PEM 提供一整套密钥管理方案，用户可以方便地使用它们。

PEM 没有涉及到的安全方面的问题包括：存取控制；报文发送忙、闲状态的保密；地址列表的精确性；路由控制；PC 机的多用户使用安全问题；报文接收的确认和接收后的不可否认性；报文的重复检测和重用。

2. RFC1421～1424

PEM 所有的规范都采用 RFC(Request For Comment)的形式给出，RFC1421～1424 包括了 PEM 的各个方面的内容：

RFC1421(前身为 RFC1113)详细给出了报文的加密、签名、封装的操作流程；

RFC1422(前身为 RFC1114)规定了基于证明的密钥管理方法(针对公钥匙体制)；

RFC1423(前身为 RFC1115)给出了目前 PEM 所支持的算法、操作模式、标志符；

RFC1424 提供密钥证实方法以及与之相关的服务。

PEM 本身并不是针对某一类型的密码体制的，事实上，PEM 既支持非对称密码体制(也称公钥匙密码体制)，也支持对称密码体制(也称传统密码体制，私钥匙密码体制)，只不过在采用对称密码体制时，PEM 将不提供发起方的不可否认服务。

二、PEM 的信息处理流程

总的说来，PEM 的信息处理流程包括两个阶段：

●报文处理阶段，这主要包括报文文本的标准化、安全服务处理以及编码过程，最终形成报文体。在这一阶段中，由于要用到接收方的公开密钥，因而将不可避免地出现身份证明的验证问题。

●报文的封装，在这一阶段，将根据安全服务中用到的一些参数生成报文头，并将报文头与报文体进行封装。

1、报文的安全服务处理

如果用户希望通过某种安全服务将一报文 m 送给他方，那么其数据处理流程为

Transmit－Form = Encode(Encrypt(Canonicalize(Local－Form)))

其中 Encode、Encrypt 和 Canonicalize 为处理过程，Local－Form 是 m 的最初形式；Transmit－Form 即为生成的报文体。

由于操作系统以及机型的不同，m 的最初形式 Local－Form 在不同的情况下是各不相同的。

Canonicalize 过程的目的就是要完成报文文本的标准化，具体说来，这一过程要完成的工作有：将文本转化成 ASCII 码的形式；采用回车换行符(CR，LF)作为文本行的分界符。

Encrypt 是安全服务实施的具体过程，根据用户的不同选择，PEM 提供三种类型的服务。

(1)ENCRYPTED 服务，这种服务包括对标准文本的加密、签名和编码过程。

(2)MIC－ONLY 服务，这种服务包括签名和编码两种处理，MIC 即 Message Integrity Check。

(3)MIC－CLEAR 服务，它只包括签名处理。显然，在这种情况下接收者收到这样处理后的报文不需任何 PEM 软件就可以查看报文内容。而在 MIC－Only 型服务中则需要依靠专门的 PEM 软件才能做到这一点。

2、报文的封装

封装过程主要是将一些重要的信息以报文头的方式添加到报文前面(这一点类似于 RFC822 规定的邮件头)，便于接收者对报文进行解密、验证签名和发送方身份。PEM 采用 RFC934 定义的机制来对报文进行封装。

一般说来，经过安全处理和封装后的报文形式为：

—BEGIN PRIVACY－ENHANCED MESSAGE—(报文上边界，标志着报文的开始)

封装头

空行(用以区分报文头和报文体)

封装体(即前述的 Transmit－Form)

—END PRIVACY－ENHANCED MESSAGE—(报文下边界，标志着报文的结束)

三、PEM 的密钥匙管理

PEM 的密钥匙管理是就公钥匙体制而言的，这里所说的密钥匙管理是指密钥匙的公开部分的管理，它必须保证任一用户获取的其他用户的公钥匙的正确性，并且能够让用户验证这一点。PEM 采用的是一种分级证明的管理方法，在这一点上它与 CCITT 的 X.509 相兼容。PEM 将整个 Internet 分为四级。级与级的关系是，每一级都只能从相邻的上一级得到它的“身份证”。该证明由上一级签过名，用户可以通过上一层的公开密钥匙来对下一层的“身份证”进行验证。一般说来，这样的一个“证明”的成员包括：版本号、序列号、签名(包括算法 ID 和参数)、发布此证明者名字、有效日期、证明的对象、证明对象的公开密钥匙。

这具体四级是：

IPRA——Internet Policy Registeration Authority

PCA——Policy Certifying Authority

CA——Certifying Authority

USER

1. IPRA

IPRA 在整个 Internet 中只有一个，它的职责是负责建立起 Internet 全局性的政策：证明每一个 PCA 的身份，并发给它们证明；保证 PCA 都遵守 IPRA 的政策，IPRA 将由一个国际性、非盈利组织 Internet Society 负责管理。

2. PCA

每个 PCA 都有自己的用户或组织的登记政策，它的身份由 IPRA 来发布。一般说来，PCA 的数量不宜过多，不同的 PCA 应当在本质上不同于其它 PCA 的政策。每个 PCA 在向 IPRA 申报身份并要求给予证明时，它应当同时附送上一份该 PCA 政策的文档。该文档应包含 PCA 的名字、服务的 CA 对象类别、将采用的安全服务类型及方式、身份证明的策略、身份证明废除管理策略等。

3. CA

CA 是用来对用户或子组织来分发身份证明的实体，它可分为三种类型：

(1)组织性 CA，即参加该 CA 的用户都同属于某一组织，比如商业性的、政府性的、教育方面的等等。

(2)地域性 CA，这种 CA 所面对的用户一般以行政区域来划分。

(3)隐蔽 CA，这种类型的 CA 是专门面向那些不愿公开自己身份的用户的。

密钥匙管理的内容包括密钥匙的建立、存储、验证和废除。

用户密钥匙的建立实际上是一个用户与 CA 之间的一个请求和回答过程(回答实际上就是“身份证”的发布)。用户在产生了自己的密钥匙对(包括秘密密钥匙和公开密钥匙)后，他就可以向 CA 发送一个请求。该请求实质上就是一个有很多部分都空白的 PEM“身份证”，为安全起见用户必须具有两个用户签名。CA 收到后，就对该请求进行验证，若正确，即可向该用户发送“身份证”。

“身份证”的验证(也即密钥匙的验证)通常发生在发送或者接收报文的时刻。

如果用户 A 希望向用户 B 发送一份报文，在对报文进行安全性处理前，A 必须验证所得到的 B 的“身份证”(除非 A 对此确信不疑)，A 可以通过使用负责发放 B 的“身份证”的 CA 的公钥匙来做到这一点。

如果 A 对该 CA 的身份也发生怀疑，他可以向相应的更上一级的 PCA 进行确认，如此反复，直到他能确认为止。而对报文接收者来说，为了验证所收到的报文的正确性，他必须对报文中的发送者的身份进行验证，方法同上。

密钥匙管理的另一个重要的方面是废除身份证表的管理。如果用户感到他的秘密密钥已经受到威胁或有别的不方便时，他就可以向合适的 CA 申请废除旧身份，并申请新的身份。从这以后，别的用户在给该用户发送报文时，就不应再使用该用户旧的公

开密钥匙了,CRL 管理应当具有这种功能。PEM 采用了 IPRA 集中存储 CRL 的方法,所有的 CA、PCA 以及 IPRA 发布的 CRL 都将被储存在一个数据库中。用户可以通过自动方式在验证他人的身份时访问该库,也可以单独按一定的规则访问该库,所有这些都是以请求和响应的方式来完成的。

四、PEM 支持的算法

目前 PEM 所支持的算法比较有限,具体说来有:

1、报文的分组加密算法,PEM 支持的是 DES 的 CBC(Cipher Block Chaining)模式。

2、MIC 算法,PEM 支持 RSA - MD2(Message Digest2)和 RSA - MD5 算法。

3、数据加密用密钥匙(DEK)的传送,PEM 采用 DES 的 ECB(Electronic Code Book)模式来进行加密。

4、公钥匙体制,PEM 支持 RSA 算法。

目前,PEM 标准尚处于实验阶段,总的说来,PEM 还不够成熟,一个称为 pem - dev 的 Internet 自由讨论小组仍然在对它进行讨论。PEM 支持的算法也还不够安全,可能是政府的原因,PEM 的分组加密算法还是采用了 DES。而单纯的 DES 算法(密钥匙为 56bits)已经受到了差分分析的强有力的攻击,已被认为是不安全的算法(密钥匙量太小)。在 PEM 的实现上,美国已经出现了两种基于 PEM 的试验性产品,即 MSU 的 RIPEM 和 TIS(Trusted Information System)的 TIS/PEM。

(第 1 期)

Web 不光用于 Internet

这些技术看起来很有发展前途,或至少是可以的,但像数据通讯设备 DCE、客户机/服务器和以 PC 为基础的查询工具之类的技术,甚至在它们真正能实用之前便开始不受人们的青睐。相反,Web 却似乎日益引起人们的关注。

目前,已有一些 Web 工具,将来可望出现更多的 Web 工具。使用 Web 技术的最重要原因是:

—有为各种各样用户平台用的 Web 客户机;

—不同的服务器不需要用不一样的客户机。

因此,在 Web 浏览器以及甚至可用于能支持图形屏幕的几乎任何一种计算机平台的自由件方面,正在形成一个很大的市场。

相比之下,在可能用于一家公司的所有各种平台上要得到 DCE 支持,或许倒是相当难的。即便是能得到 DCE 工具的情况,但要开发用于所有各种平台的客户机软件也可能是一项相当艰难的任务。

这种情形甚至已使许多家公司下决心禁止使用不支持 DCE 的系统。

若采用 Web 方法,用户就不需要像用大多数的其它存取技术一样,存取每一个服务器要用不一样的客户机软件块。用来存取最新迪斯尼影片 Home Page 的浏览器,也能用来寄存该机构内的一个输入地址。

现已有一些基于 Web 的系统,用来存取个人履历、配置路由器、修改定时卡、寄存输入地址。查询电话号码、与一个 SNMP 管理站接口以及甚至有配置 XWindow 服务器的基于 Web 的系统。

一些新的 Web 特点,诸如 Java 可卸载的例行程序,将提高 Web 系统的灵活性,并增加了将 Web 技术用于很多其它场合的可能性。

但这种发展趋势也存在着很多问题。当前,Web 还没有安全性标准。所以,尽管 Web 系统很快就会上市,但在它实用之前教授们仍不太想用它来更新注册计算机上的学生成绩。

了解加入网络联系的某人就意味着对人的一点信任,然而,Web 系统在某种情况下便能大大降低所需要的对人的信任程度。

我认为任何一种联网技术都不能解决世界上所有的联网要求;我还认为任何一种接口技术对所有的应用来说也未必是最好的。所以,人们不能指望 Web 有很好的用于某些应用的一些性能,比如用一个路由器观察交通情况的实时显示。并且人们在试验和使用 Web 技术来代替编某些专用客户机程序方面也有一些曲解。

(第二期)

Web 用户知多少

由于 Web 正变得越来越易于使用，致使许多并无多少 Web 经验的人也纷纷开始使用这一网络。

这是美国佐治亚技术研究所图形视频化及可用性(GVU)研究中心第四次 World Wide Web 用户调查所得出的结论之一。

这项调查是 GVU 于 1995 年 10 月～11 月在 Web 网上进行的。此次调查还发现，非美国用户的百分比正在增加。与此同时，当前已有更多的妇女和专业技术人员也开始使用 Web 网络。

与前几次的调查相比，第四次 World Wide Web 用户调查选择了更为广泛的用户群体。

接受调查的用户一共有 2.3 万人——几乎是 1995 年 4 月份第三次调查人数的两倍，是 1994 年 1 月份第一次调查人数的 15 倍。

用户可以很方便地从 GVU 的 Web 网点索取到这份调查报告，此次调查仍以美国用户为主。

GVU 宣称，目前他们正在着手考虑下一次的调查。第五次 World Wide Web 用户调查计划于 1996 年 4 月份开始，调查组的日常工作将在新西兰的一个 Web 网点进行。

另外，GVU 还准备把第五次调查的某些重要结论翻译成包括希伯来语、日语、意大利语以及西班牙语在内的其他国家的语言。

这次调查亦存在着一定程度的局限性，接受调查的人多为那些较频繁使用 Web 的用户。尽管如此，此次参加调查的美国 Web 用户的身份类别与 1995 年早些时候 GVU 对美国和加拿大 Internet 用户所做的那次 CommerceNet/Nielsen 随机电话调查的用户身份大体相似。

以下是这次 World Wide Web 用户调查的部分结果：

●76％的被调查者来自美国、10％来自加拿大和墨西哥、8％来自欧洲、2％来自澳大利亚和新西兰、仅有 1％多一点来自亚洲。

这次与上次调查相比，非美国用户的数量略有增加。在上次调查中，80％的用户来自美国、9.8％来自欧洲、5.8％来自加拿大与墨西哥。

●尽管越来越多的妇女正在使用 Web，特别是在美国，但男性仍是 Web 用户的主体。总的来说，71％的 Web 用户为男性、29％是女性。在美国，67％的 Web 用户为男性、33％是女性。在欧洲，近 90％的 Web 用户为男性、仅有 10％多一点是女性。

●60％的被调查者使用 Internet 不到一年、27.7％使用 Internet 不到 6 个月。自从第三次调查以来，使用 Internet 在 1～3 年的用户的百分比已大幅度下降，即从过去的 26.9％下降到目前的 11％。

●所有被调查者的 31％来自教育领域、29％来自计算机领域、19.9％为专业技术人员、10.2％为公司管理人员。

在教育领域和计算机领域中的用户，欧洲略高于美国(在欧洲分别为 33.8％和 33.6％，在美国分别为 30.6％和 29.1％)。专业用户群体，美国的用户略高一些(美国为 20.4％，欧洲为 16.4％)。

●在使用 Web 的过程中，用户报怨最多的问题是：速度慢、寻找信息比较困难。

●被调查者使用 Web 频次最高的是：替换软件、查找参考资料、阅读电子新闻、以及寻找产品信息。

●Web 用户的平均年龄为 32.7 岁，低于上一次调查的 35 岁。平均说来，欧洲的 Web 用户比美国的年轻。欧洲为 29.7 岁，美国为 33.2 岁。

●此次调查结果表明，Web 用户的平均年收入有所下降，即从上次调查的 6.9 万美元下降到此次的 6.3 万美元。美国 Web 用户的平均年收入略高于欧洲，分别为 6.47 万美元和 5.6 万美元。这说明，在欧洲的 Web 用户中，学生占了很大的比例。

GVU 第四次 World Wide Web 用户调查的全部结果，可从 http://www.gatech.edu 上获得。

(第三期)

Java 走红但决非完美无缺

Java 刚刚推出之时，人们只是把它作为一种特殊的程序设计语言，为 Sun 微系统公司所开发的电视机机顶盒偶然编写一些小型应用程序。

分析家们曾预言，这一语言的不断演化及成功的市场推销，将会打破 Microsoft 公司独霸软件市场的一统天下。它将会把计算机的计算能力带给每一个人，并可为程序设计带来革命化的变革。与此同时，Java 语言还能够胜任许多 Smalltalk 和 Xerox-PARC 无法胜任的工作。

然而，实际情况究竟如何呢？事实上，尽管 Java 是一种极好的程序设计语言，但它并不像人们所期望的那样十全十美。

以下，让我们来对这一程序设计语言做一个较为深入的探讨。

———Java 语言允许程序设计人员把相当数量的功能集中在一个非常小的程序包中，这种程序包可运行在高度分布式网络中的任何地方，这也正是 Java 语言的最大优势所在。另外，这一语言有力地支持了 Sun 的网络技术，实现了 Sun 对网络技术语言的提交承诺。

——Java 语言允许 World Wide Web 网点的创建者向这一网络添加新的交互功能。目前从理论上讲，向各现存 Web 网点添加交互功能是完全可行的，即只需你自己来创建一个解释程序，并能把它提交给 任意一位潜在的用户。但在实际实施过程中，这一添加工作是相当繁琐的。然而，Java 语言简化了这一添加过程，这也是 Java 可成功进入市场的关键所在。

Sun 公司首先使用了这一语言，并在解释程序中建立了一个浏览程序，即 Netscape Navigator。

Java 是一种类似 C 的语言，而不是那种类似 Basic 或类似 Pascal 的语言。目前，类似 Basic 和类似 Pascal 的语言已得到具有不同程序设计水平的用户们的广泛使用。而类似 C 的语言特点，是 Java 语言的一大缺憾，致使这一语言的程序设计对用户提出了较为苛刻的要求，即使是很熟悉 Web 的人，要想彻底掌握这一语言，亦决非一件易事。但是，Java 语言的推出，意味着各种 Web 程序设计技术将会得到长足的发展。其中包括商用程序设计、公司应用开发、以及娱乐程序设计等。预计，开发 Java 应用可能会成为各 Web 网点今后赚钱的重要源泉。

Java 语言的良好功能，可使人们开发出数以百计的需要时可以呼之即来，不用时可以随手丢弃的数字处理程序与电子表格，即用户只需点击鼠标器便可把它们调出来加以使用，不再使用时可随时将它们抛弃。另外，对这种数字处理程序与电子表格的使用，用户每次只需支付很少的费用，从而可不必花大钱去购买和安装 Microsoft 公司相比之下显得十分笨拙的同类软件产品。

事实证明，无论你使用什么样的语言来编制字处理程序和电子表格，都不是一件轻而易举的事。加之某些设计方案上的缺乏，程序量往往大得惊人。

Java 语言可向用户提供一种新的交互特性，这一特性与我们现已拥有的交互功 能不同，这种新的交互性是我们在 PC 软件中难以得到的。这里指的主要是那些看上去很小但程序量却不小的人机交互环境。由于功能太小以致于人们不愿花大力气去设计、制造与销售它们。例如某些专用计算器、智力卡片、各种活动表格及计算机购物工具等。所有这些人机交互设施若能使用 Java 的这一新的交互特性，均可快捷地得以实现。

Java 确实是一种极好的程序设计语言，但用户只有很好地发挥它的交互特性时，才能充分利用这一语言最重要且最昂贵的资源——熟练的 Java 程序设计人员。

（第三期）

新兴 Internet 电子支付系统

货币、现金支票、商品券等传统支付方法在计算机内部无法使用。为了能够在 Internet 上进行支付，特别是能够通过 WWW(环球网)进行支付，人们正在致力实现新的电子支付系统。

本文将对 Internet 这一前景广阔的新用途，以及刚面世的六种商用的 Internet 支付系统进行介绍。

支付系统简介

无论是数字方式还是其他方式，支付系统都可分为两大类，即借方(debit)和贷方(credit)的。借方指使用现金、贷方指进行信贷。在现金系统中，首先要把现金调拨进去，然后才可以从这里花钱。而在信贷系统中，可以先买东西然后再要求付款。例如使用黄金、纸币、旅行支票支付的便是现金系统。也有通过 ATM(自动提款机)使用现金卡进行支付的。而使用支票、赊帐、信用卡等，则是信贷(信用)系统。

就像现金和信用卡在现代商业环境中并存一样，它们也将在数字世界中并存。所谓数字现金就是支票和无记名债券(由银行及其他机关发行)的数字版。用户从银行购入这些票据(银行把它们作为借方系统运用)，然后可以把它们变换为实物。用户也可以把这些票据进行数字式复制，但银行只对票据的每一个编号兑换一次现金。

数字式信用和商业领域使用的信用系统类似。主要的差别在于采用数字时间戳和数字签名。通过这些，赋予系统以监督和责任的功能，以取代文件类的处理(这在数字世界中并不存在)。

支付人通过这样系统生成包含有交易的内容、支付人和收取人的名字、交易日期、以及应付的金额等内容的凭证(表示交易的传票和证据等)的记录。支付人使用自己个人键码对这样凭证进行签署。凭证的收取人用公开的键码便可读这一记录，并对其进行签署，这样便可确认个人键码所有者所承担的支付义务。然后，收取人向清算系统提出该凭证，便可取得用以收款的法律根据。

电子支付系统的社会基础

现已存在电子支付系统的社会基础。主要信用卡公司(如 American Express、Master Card、Visa、Discover)、ATM 网络、以及 ACH(自动清算中心)便是这样基础。对信用卡业务来说，有三种处理系统。一是银行，它给顾客以信用卡并进行请求。二是第三方的处理公司，它向信用卡加盟店提供认证和收款业务。三是像 Visa 这样的国际网络，它把进行收款的处理业者和银行联系在一起。这些系统虽很复杂但已完善，几乎可向所有场所普及。加盟店支付的手续费为交易总金额的 2% 至 3%，另外每笔交易再加收 20 美分。

一些信用卡公司已向加盟店提供使用 Internet 的服务。信用卡系统已真正具有国际性，它已能适应于用各种各样通货进行的交易。这些都能很好地纳入银行系统中。Internet 的巨大优点已经表现在信用卡系统中。

所谓 ACH 是美国银行之间的一种机构，通过它，地方银行向数据库提出支付，第二天之前联邦储备局便得以拨款。

这是一种通过户头转拨的收费支付方式。ACH 交易收费低廉(每笔不到 15 美分)，而且能用计算机进行处理。ACH 只能在美国银行户头间工作，但这种方法被广泛用于在线的支付清算业务。

通过现金卡网络，既可用 ATM 从自己的户头上取出现金，又可作为支付拨到别的银行去。银行对这种业务每笔支付 50 美分。银行在进行支付前既要求有实物的卡又要求有密码(也叫 PIN)。现在安全性上还存在问题，解决了以后便可利用网络进行直接的在线支付。

个人和民营企业将保持自己的顾客户头，不妨碍从这些户头进行支付。几乎所有的在线服务都可用这种方法向提供服务内容的公司进行支付。如果这些在线服务机构提供对使用者户头的服务器，这种系统也许就能承担重要的银行业务。

采用客户/服务器方式

在线的支付处理通常同三方面有关。顾客进行支付，加盟店接受支付，银行进行会计处理并确认从顾客那里把款拨到加盟店户头上。在对等通信系统中，用户起到顾客和加盟店两方面的作用。支付服

务系统虽然从法律上说不能视为和银行一样，但它可起银行那样的作用。

顾客将运行客户机软件。有的是像 Mosaic 那样的 WWW 浏览器，有的是带有 Netscape 和 S－HTTP（安全超文本传输协议）的 Mosaic 那样的有密码化功能的浏览器。也许还有使用专门的支付客户机。

加盟店为了支付请求和处理，要在服务器上运行加盟店软件。在许多情况下，加盟店软件同 WWW 服务器相结合。支付服务器在网络上是银行 POP（存在点）。在进行实时交易时，加盟店把信息送到支付服务器，在这里对支付进行认证然后往加盟店户头进行拨款。

安全性和私人秘密是必须解决的问题

安全性在所有数字支付机构中都是非常重要的问题。用以证明确是用户本身最一般的方法是要求密码。由于消息在 Internet 上传送时很容易被读走，所以几乎在商用服务中在发送密码前都进行了加密。采用新一代 WWW 浏览器进行这种加密。作为这种浏览器有使用 SSL（安全插座层）加密协议的 Netscape 和 Mosaic 派生品（使用 S－HTTP）的。

问题在于加密的密码，重复使用两次以上也不安全。最后，也许用户只能使用硬件标志的方法。这就是在普通信用卡的大小上，作成唯一一次的密码，并使其加密以保持安全。

为了确保安全，金融消息的内容（支付、信用卡号码、或数字署名）都要保密，此外还要使消息不被篡改。在现在正在使用的几乎所有系统上，都保持有用以检查监督交易的某种凭证文件。为了发展在线支付系统，必须有能和这种文件相匹敌的功能。能进行加密的现有机构，能提供这种功能。

保守私人秘密也是同安全性有关的问题。在当今庞大数据库时代，许多人都在想这一问题。大家都同意在数字金融交易中应和现金交易中一样，采取匿名原则。任何人在使用现金时，无关的人都不应该知道。使用现有的数字加密技术便可达到这一目标，但已经使用这一技术的只有一部分电子支付系统。

Internet 上用的电子支付系统纷纷面世

美国《BYTE》杂志对 6 种商用电子支付系统进行了调查。它们是 Cybercash、Digicash、First Data/Netscape、First Virtual、Open Market、Wave Systems。这里不包括 Visa/Microsoft、Master Card/Netscape 发表的共同事业。这两家无疑将是今后支付服务市场的两大势力，但它们都是在 1995 年下半年才开始服务，因此现在还不好对它们说些什么。下面对这 6 种在 Internet 上使用的电子支付系统进行评介。

Cybercash 它以“银行就是顾客”作为座右铭，希望所有交易都直接送往实际银行。现在顾客在接受服务时还无法通过 Cybercash 同银行对话，所以 Cybercash 正在同 WellsFargo 银行进行这种能对话的试验，很快就能提供正式服务。

Cybercash 的软件作为同银行的界面有很好的功能。它将通过提供可移植于家庭银行用的 ATM 来实现。借方用的版本已被证明在资金移动、票据支付因而也就在对等通信支付方面拥有卓越机构。但是，早期的信用卡版本稍微差些。顾客要对每次交易输入信用卡传票，而且没有预约申请机构。和使用卡时一样，在 Cybercash 中由加盟店承担欺诈交易的责任。对 Cybercash，《BYTE》的评价是，对一次性的目录销售它是“良好”的，对信息销售它是“普通”的。

Digicash 它在信息服务领域是最为革新的、也许也是最为重要的。它的创业者 David Chaum 曾获发明名为 E－cash 的数字出纳形式的专利。它能够保守顾客的私人秘密。Chaum 认为：“已经进行的支付如果都用电子记录下来，电子支付系统就没有必要侵犯私人秘密。这一概念非常重要，因为它也可以说是一种人权问题。”

E－cash 的软件因方便而受到欢迎。不论在地球上哪个地方，都别想付出高的费用就可得到私人秘密，这意味着它是不论谁都可进行交易的对等的支付机构，因而 E－cash 是有利个人的东西。

由于还没有同 E－cash 系统签订合同的银行，无法评价它的适用性。但今后一定会引人瞩目。

First Data/Netscape 美国最大的信用卡处理公司 First Data 和当前最受人注意的 WWW 软件厂商之一 Netscape Communication 公司，为了提供信用卡认证服务而进行了合作。这一机构只不过是对现在使用的借助电话进行的信息用卡支付系统，给予一点点修正。不是用电话把信用卡号码告诉加盟店，而是改为顾客在 HTML（超文本标记语言）平台上键入号码。这样，客户机便可利用 Netscape 中含有的加密功能，将这一号码送给加盟店的服务器。这一产品现在正通过 Marketplace MCI 而得到使用。Netscape 的服务器和 First Data 的处理服务，质量都很高，二者进行合作自然会产生新的附加价值。

但是这一产品需要专用的电话线，所以要多花一些费用。如果是拥有加密功能 的 Netscape 或 S－HTTP 的 WWW 服务器的加盟店，则可安装 500 美元以下的像 IC－Verify 这样便宜的卡认证软件，然

后同自己选择的信用卡处理公司进行合作。这时，用户已经把信用卡号码送给加盟店。这一产品的机构简单，但保留了现在信用卡支付系统的安全性方面缺点。显然，它只是过渡性的产品。《BYTE》对它评价为"普通"的。

现在加盟店和顾客都对 Netscape 和 Master Card 的共同事业寄以更大希望。在这一系统上，Master Card 将在 Internet 上设置支付服务器。通过它就用不着让加盟店使用专门的电话线。此外，通过在 Internet 上设置支付服务器，署名的信用卡传票由于认证时加盟店不用知道顾客的信息，故可直接送往支付服务器，这便增加了顾客的安全性。

First Virtual 是采用"买前先试"方式的独特的信用卡处理公司。已经运用中的这样系统，基本上是为出售信息等的"软"商品的厂商而设计的。公司取名 Virtual(虚拟的)是指它是采用独特的公司组织形式。该公司主任级的人员全都在各自的州从事工作，靠电话联系和 Internet 服务器的维护，它也可以承包给其他州的公司。这样的虚拟组织和简单的自发支付系统，据说非常适合于 Internet 上的分散环境。

First Virtual 的服务，对采用信息卡处理交易的加盟店来说是简单的方法。特别是它不需要 WWW 浏览器和加盟店处理的户头。因此花在加盟店上的初始费只要 10 美元。

不过这一系统虽然也有密码和强大的电子邮件功能，但顾客用起来有时还是有点不方便。支付的安排不确定，署名登录机构虽也自动化但动作笨拙。因此，"虚拟"这一概念并不反映实际的服务机构。关于它在 WWW 信息销售方面的适合性，《BYTE》对 First Virtual 的评价是"普通"的。

Open Market 它是专门建立"Internet 店铺"和支持它用的支付服务的新公司。系统完全基于 WWW，100% 地使用 HTTP 标准。系统现在利用 Open Marketplace 的 WWW 服务器在内部使用。

它和上述其他厂商不一样，Open Market 不仅自己开发，而且还是对结算和招揽顾客等积极开展业务的服务公司。Open Market 的服务器是唯一的能提供顾客服务和预约销售会计、总计请求的货款、不同等级安全性、以及企业间会计等功能的支付服务器。

它有使用便利的优点，但顾客对所有交易都要用支付服务器也是个缺点。《BYTE》对它适用性的评价为"良好"的。

Wave Systems Wave System 的 Wave Meter 现在正处于 β 试验阶段。它是基于硬件的，作为对数字支付的手段，采取了同其他厂商完全不同的方式。用户在自己的计算机上装上它的芯片。如果在芯片上拨出款项，则芯片便可对其进行计算。

Wave Systems 已成立 5 年，股票已公开上市。芯片厂 National Semiconductor 董事长 Peter Sprague 是它的创建者。他声称，系以自动售货机作为模型。Wave Meter 可以用于出售信息、软件使用许可、或软件使用时间。

Wave Meter 还可以用以测量 CD－ROM 或卫星或 FM 广播那样的媒体所提供的加密了的信息的量，适于对它进行解密。但是，复杂的 WaveMeter 系统不能同中心的支付服务器相竞争。因此，《BYTE》只对它的有用性，评价为"不好"的。

（第九期）

13 种防火墙产品评介

俞鼎昌

《网络世界》最近考察了 13 种控制对 TCP/IP 网络访问的防火墙产品，本文有助于你对它们的认识并能帮助你选择自己适用的产品。

Livingston 公司的 Firewall IRX 和网络系统公司(NSC)的 The Security Router 是基于路由器的低档防火墙产品，它们适用于简单安全策略的场地。

Trusted 信息系统公司(TIS)的 Gauntlet 和 Network－1 软件和技术公司的 FireWall/Plus 为用户提供了自己动手构筑防火墙的素材。

Digital 公司的 Firewall for Unix 和 Check Point 软件技术公司的 Firewall－1 是最容易配置的产品，并且 Firewall－1 在由一个界面管理多个防火墙以及在混合数据包过滤与应用代理技术上处于领先。

Border 网络技术公司的 BorderWare 提供了一套

最完整的将防火墙与 Internet 服务器合而为一的解决方案。

Milkyway 网络公司的 Black Hole 提供的应用代理防火墙最具创造性，而 Harris 计算机系统公司的 Cyber Guard、IBM 的 Secured Network Gateway (SNG)、Secure 计算公司的 Side Winder 和 SOS 公司的 Brimstone 都非常值得信赖。

Network Translation 公司的 PIX 将快速高效的网络地址转换(NAT)与某些防火墙的功能合并成为一个功能强并且容易配置的套装软件。

上述 13 种防火墙产品自推出迄今都有重大的改进，目前，几乎所有的产品都把各种不同的防火墙技术结合在一起。

防火墙路由器

Livingston 的 Firewall IRX 和 NSC 的 The Security Router 是将路由器和防火墙系统合并构成的系统，也是包括防火墙功能主要的网络路由器。它们是通过记录与安全有关的信息(如对当地主机攻击的信息)而扩大了简单路由器的功能，它们也可在其它协议上进行有限制的过滤。Firewall IRX 只限于在 NetWare 的 IPX 协议上使用，而 NSC 的 Security Router 还可在 AppleTalk、DECnet、XNS 和 VINES 上过滤，Firewall IRX 仅限于过滤和监视网络信息流，而 Security Router 还提供安全的 IP 管道。

这两种产品的不足是缺少状态信息，即不能在以往的信息基础上决定通过还是放弃经过它们的信息流，因而限制了这些产品所能支持的安全策略的多样性和效能，特别是对象 User Datagram Protocol 用户数据协议(UDP)这样的无连接协议。防火墙和有些 TCP 协议如 File Transfer Protocol(FTP)等工作时也需要状态信息，FTP 使用两个连接传输数据，Firewall IRX 和 The Security Router 都单独检查每个数据包而不需要以前的数据包任何信息，它不能对使用无连接 UDP 的 Domain Naming System(DNS)通过防火墙作出反应而只能回答 DNS 的访问。如果用户打算大量使用象 Network File System(NFS)这样的基于 UDP 的服务扩大进入 Internet，无状态信息的防火墙产品则不能工作。

Network－1 软件和技术公司的 FireWall/Plus 是在路由器作为防火墙方式上的改型，是一种革新的防火墙。它不转发数据包，而是在两个以太网界面间搭桥让包通过，并且对任何更高层的协议，它都是不可见的。FireWall/Plus 考察它所接收到的每个以太帧，并在帧本身的内容如帧类型、媒介访问控制地址、子域或长度或帧中高层协议数据等来决定让帧通过还是放弃。

FireWall/Plus 可用来对非 TCP/IP 协议进行简单的过滤，但最大的用处还是对运作在 IP 顶层的协议。因为它包括有对大多数基于 IP 的协议和安全方案有预先制定好的规则，它不仅能处理传统的 TCP 和 UDP，还能处理其它在 IP 上运行的协议，譬如象 Open Shortest Path First 转发协议，同时 FireWall/Plus 也能存储某些类型的状态信息以便安全地处理象 DNS、NFS 和 FTP 这样的协议。

Network Translation 公司的 Private Internet Exchange(PIX)是一种特殊类型的包过滤路由器，它执行 NAT 并且还内置许多安全功能，PIX 有助于机构将它们的内部 IP 地址隐藏起来，PIX 的安全功能能对 FTP 等协议保留一些状态信息，并且还包括基于 TCP/IP 的协议如 Telnet、SMTP 或者 Network News Transport Protocol(NNTP)的规则，而且还有 IP 管道功能。

过滤器的灵活性

Check Point 的 Firewall－1、Harris 的 Cyber Guard 和 IBM 的 SNG 使用了包括应用代理、线路及网关和简单的基于 IP 的包过滤多种技术的组以实现网络安全策略，这 3 种产品能让网络经理不必改变客户机系统上的软件即可支持彻底开放的内部环境，从而有最大的灵活性。虽然它们既支持应用代理和线路网关，但因为它们重点在包过滤技术，所以这 3 个产品在这个领域是最强的。

Gauntlet 是由具有很久防火墙开发历史的 TIS 公司推出的，它包括有 TIS 第二代具有简单的综合管理用户界面和其它专利工具的免费工具包，TIS 是提供其软件全部源码的唯一厂商。

SOS 公司的 Brimstone 防火墙软件包比原版收集了更多的公用工具，尽管 SOS 确实增加了某些在用户界面和监视方面颇为知名的专利软件，而 SOS 的主要贡献还是在其防火墙产品中对软件的收集、包装、编产品文档和产品验证等方面，这种工具包的方法鼓励网络经理们改进他们自己的防火墙产品。

如你不想知道 Unix 或网络安全和安全防火墙配置的详细知识，可以看看 Milkyway 的 Black Hole、Digital 的 Firewall for Unix、Secure 计算公司的 SideWinder 和 Border 公司的 Border Ware 防火墙服务器。这些产品通过减少可能的选项简化了构筑防火墙工作，它们依靠应用级代理和线路网关放行大部分常用的 TCP/IP 应用程序，为了简化管理用户界面，该软件设置了一些其它限制，譬如除 Black Hole 外都限制在通常以太网卡支持的 IP 界面的数目上，

这也有助于简化用户界面。

这些产品也涉及其它常见的系统管理任务，譬如后备、报告、记录和系统配置成一个用户界面等，原则上都能把你从 Unix 的命令行中解放。

防火墙界面

防火墙最大的市场是在保护公司网络不受公用网如 Internet 的侵扰上，面向 Internet 的防火墙一般有两个 LAN 界面：一个为网络的不安全方（有时称为"脏"或"红"方），一个为网络的安全方（有时称为"洁"或"兰"方）。我们考察的防火墙都至少支持两个 LAN 界面，很少有仅支持两个界面的。

受仅支持两个界面限制的配置对兼职的安全经理来说有个最大优点，即用户界面关于什么是被允许的、什么是被过滤的非常明显，譬如在 FireWall/Plus 中网络内侧用天使图标表示，而网络外侧用魔鬼图标表示，Digital 的 Firewall for Unix、Side Winder、PIX、Gauntlet 和 Cyber Gaurd 都有相同的配置限制即两个界面、有很强的 Internet 环境面向性。

Border Ware 允许有 3 个界面，但也有相同的严格定义：一个是脏的不安全的；一个是洁净的内部用的；另一个是用于不被信任的可访问 Internet 服务器（通常称为非军事区）的子网。

对具有多个防火墙、多机构、多 LAN 或其它信任和不信任网的更为复杂的环境来说，两个界面是不够的。更多的界面当然带来更多的复杂管理界面和配置选项，从而为构筑多种安全策略的防火墙提供更多机会。

Black Hole、SNG、Firewall－1 和 Brimstone 都支持多界面，但 IBM 的 SNG 仅在 SPARC 平台上支持。

Firewall－1 的多界面思想甚至进一步扩展了单一平台的限制，它的管理用户界面能让一组带有许多 LAN 和 WAN 界面的 Firewall－1 系统和路由器作为一个具有单一安全策略和记录点的实体而被管理，Brimstone 提供一个相似的但不太全面的功能。

通过防火墙隔开

我们测试的每个防火墙在处理通过防火墙的访问上方法都略有不同。一般来说，外部访问内部服务采用简单地关闭，防火墙的作用象个单向阀，让内部用户向外发送信息流而禁止外部任何信息流进入。有些防火墙提供特殊通孔准许外部特定的系统与内部的特定系统连接，譬如外部的 NNTP 与内部的 Usenet 新闻服务器相连接。

若你仅需要的是一个单向阀，则差不多任何一个防火墙都能支持你的安全策略，若你有更复杂些的安全策略，则你需要更多一些的对防火墙鉴别的知识了。

我们将产品粗略地分成两大类：一类基本上是基于 IP 地址的产品，另一类是基于用户认证的。第 1 类产品一般更关心特定用户进来的 IP 地址是什么而没有严格的认证要求，第 2 类产品在用户与通过防火墙的访问之间有严格的纽带关系，一般认为对非法用户到处游荡更为困难，也还有将这两种或多种技术混合的产品，它们更为吸引人。

Firewall for Unix 和 Border Ware 有最严格的访问要求，一切认证的访问必需使用一次性口令。譬如你欲让厂商暂时通过防火墙诊断一个故障，你必须为他们建立一个手持的令牌或者当某个有令牌的人能对一次性口令正确回答时才让他们进行访问，所有其它认证或防火墙厂商也允许使用不太安全的重复口令机制。

如你的策略不信任所有外部的人而信任大多数内部的人，则基于 IP 的过滤可能就够了，对发自你网络内的信息流，此种过滤能工作得很好。对外部企图进入你的网络的用户，基于 IP 的过滤则是另外一码事，因为 Internet 无安全可言，没有可信任的 IP 地址，因为它们能很容易地被改变或被骗过，用户认证未必有帮助，因为蓄意的入侵者能想尽一切办法侵入现有的 TCP 会话。

对于没有基于用户认证和依靠 IP 地址的产品，是否让信息流通过我们检测的包含有路由器的防火墙有：Livingston 的 Firewall IRX、NSC 的 Security Router、Network Transtation 的 PIX 和 Network－1 的 Firewall/Plus。

Digital 的 Firewall for Unix 和 Border 的 Border Ware 在此方案上稍有变化：当向外发送信息流时所有内部用户都要在 IP 地址的基础上进行过滤，外部用户试图进入必须经一次性口令的认证。

Side Winder 的方法比较有限和含糊，它在 IP 地址基础上进行过滤，但也能对来自 WWW 的浏览器如 Netscape Navigator 的信息流使用认证。其它产品能让用户对特定的 IP 地址在某时间间隔内在防火墙上开个临时的通孔。譬如你欲通过防火墙建立一个远程登录（telnet）连接，你必须对防火墙首先用口令和用户名认证你自己，一旦防火墙看到来自特定 IP 地址的有效用户名和口令，它就让进行访问。

这种技术最好的例子就是 Milkyway 的 Black Hole 内置在 Black Hole 中的代理，在让信息流通过之前监视未授权的信息流和请求认证。这对象 Hyper Text Transfer Protocol（超文本传输协议 HTTP）和 Gopher 等协议来说特别合适，因为防火墙认证相对